INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.2111

Amendment 1
(07/2001)

SERIES Q: SWITCHING AND SIGNALLING

Broadband ISDN – Signalling ATM adaptation layer (SAAL)

B-ISDN ATM adaptation layer – Service specific connection oriented protocol in a multilink and connectionless environment (SSCOPMCE)

Amendment 1

ITU-T Recommendation Q.2111 – Amendment 1

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation Q.2111

B-ISDN ATM adaptation layer – Service specific connection oriented protocol in a multilink and connectionless environment (SSCOPMCE)

AMENDMENT 1

Summary

Recommendation Q.2111 provides assured data delivery between AAL connection endpoints in a multilink or a connectionless environment. This amendment has been prepared to allow operation over additional types of connectionless lower layer protocols and is designed to be compatible with implementations conforming to that first edition of Recommendation Q.2111 (1999).

The changes from Recommendation Q.2111 (1999) specify operation of SSCOPMCE over additional connectionless lower layers than the original publication of Q.2111 (1999). Specifically, the additional connectionless environments are:

– IP, as modified by Differentiated Services in IETF RFC 2474; and

– Ethernet, as defined in ISO/IEC 8802.3.

This amendment supersedes the Implementor's Guide published in December 2000.

Source

Amendment 1 to ITU-T Recommendation Q.2111 was prepared by ITU-T Study Group 11 (2001-2004) and approved under the WTSA Resolution 1 procedure on 13 July 2001.

CONTENTS

ITU-T Recommendation Q.2111

B-ISDN ATM adaptation layer – Service specific connection oriented protocol in a multilink and connectionless environment (SSCOPMCE)

AMENDMENT 1

Replace clauses 2 and C.1 and modify clauses 5 and 7.3.3 with the text presented in this Amendment. The differences from ITU-T Recommendation Q.2111 (1999) for these sections are marked to emphasize the compatibility of this Amendment with the original publication of this Recommendation.

Enhance clause 4 with the additional abbreviations presented in this Amendment.

Add new Annexes D (Convergence function for SSCOPMCE above IP or UDP with Differentiated Services) and E (Convergence Function for SSCOPMCE Above Ethernet)

Replace Appendix I by the Appendix I provided in this amendment.

The additional and modified text follows.

1) Clause 2

2 References

2.1 Normative references

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

[1] ITU-T X.200 (1994), *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model*.

[2] ITU-T X.210 (1993), *Information technology – Open Systems Interconnection – Basic Reference Model: Conventions for the definition of OSI services*.

[3] ITU-T I.150 (1999), *B-ISDN asynchronous transfer mode functional characteristics*.

[4] ITU-T I.361 (1999), *B-ISDN ATM layer specification*.

[5] ITU-T I.363.5 (1996), *B-ISDN ATM Adaptation Layer specification: Type 5 (AAL)*.

[6] ITU-T Q.2110 (1994), *B-ISDN ATM adaptation layer – Service specific connection oriented protocol (SSCOP)*.

[7] IETF RFC 768 (1980), *User Datagram Protocol*.

[8] IETF RFC 791 (1981), *Internet Protocol*.

[9] IETF RFC 792 (1981), *Internet Control Message Protocol*.

[10] IETF RFC 1122 (1989), *Requirements for Internet Hosts – Communication Layers*.

[10 *bis*] IETF RFC 2474 (1998), *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*.

[10 *ter*] ISO/IEC 8802-3:2000, *Information technology – Telecommunications and information exchange between systems – Local metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection CSMA/CD access method and physical layer specifications*.

2.2 Bibliography

The documents listed in this clause provide informative background information for the reader and are not normative within this Recommendation.

[11] ITU-T Q.2100 (1994), *B-ISDN signalling ATM adaptation layer (SAAL) – Overview description*.

[12] ITU-T Q.2130 (1994), *B-ISDN signalling ATM adaptation layer – Service specific coordination function for support of signalling at the user-to-network interface (SSCF at UNI)*.

[13] ITU-T Q.2140 (1995), *B-ISDN ATM adaptation layer – Service specific coordination function for signalling at the network node interface (SSCF at NNI)*.

[14] ITU-T I.365.2 (1995), *B-ISDN ATM adaptation layer sublayers: Service-specific coordination function to provide the connection-oriented network service*.

[15] ITU-T I.365.3 (1995), *B-ISDN ATM adaptation layer sublayers: Service-specific coordination function to provide the connection-oriented transport service*.

[16] ITU-T I.363.2 (2000), *B-ISDN ATM Adaptation Layer specification: Type 2 AAL*.

[17] ITU-T I.366.1 (1998), *Segmentation and Reassembly Service Specific Convergence Sublayer for the AAL Type 2*.

[18] ITU-T Q.2119 (1996), *B-ISDN ATM adaptation layer – Convergence function for SSCOP above the frame relay core service*.

[19] IETF RFC 2475 (1998), *An Architecture for Differentiated Services*.

[20] ISO/IEC 8802-2:1998, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 2: Logical link control.*

[21] ISO/IEC 15802-3:1998, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Common specifications – Part 3: Medium Access Control (MAC) Bridges.*

[22] IEEE 802.1Q (1998), *IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks*.

2) Clause 4

4 Abbreviations

Add the following list of abbreviations, alphabetically, to those already contained in clause 4:

CFI Canonical Format Indicator

CPCS-CI Common Part Convergence Sublayer Congestion Indication

CPCS-LP Common Part Convergence Sublayer Loss Priority

CPCS-RS Common Part Convergence Sublayer Reception Status

CPCS-UU Common Part Convergence Sublayer User-to-User Indication

CPI Common Part Indicator

CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CU	Currently Unused
DF	Don't Fragment
DS	Differentiated Services
DSCP	Differentiated Services Codepoint
FCS	Frame Check Sequence
FO	Fragment Offset
ICMP	Internet Control Message Protocol
ID	Identification
IDU	Interface Data Unit
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IHL	Internet Header Length
ISO	International Organization for Standardization
LAN	Local Area Network
LLC	Logical Link Control
LSRR	Loose Source and Record Route
MAC	Medium Access Control
MF	More Fragments
NCFI	Non-Canonical Format Indicator
PROT	Protocol
PVID	Port Virtual LAN identifier
RFC	Request For Comment
RIF	Routing Information Field
RR	Record Route
SFD	Start Frame Delimiter
SNAP	Sub-Network Access Protocol Identifier
SSRR	Strict Source and Record Route
TCI	Tag Control Information
TCP	Transmission Control Protocol
TL	Total Length
TOS	Type Of Service
TTL	Time To Live
VID	Virtual LAN Identifier
VLAN	Virtual LAN

3) Clause 5.3

5 General

Modify the paragraph immediately following Figure 2 as follows:

A representation of SSCOPMCE operating in a connectionless environment is shown in Figure 3. In this mode the SSCOPMCE entity operates more like a transport layer protocol and is clearly outside the scope of an AAL. Through the lower Service Access Point (SAP), a connectionless service, such as IP (IETF RFC 791 [8]) or UDP (IETF RFC 768 [7]), delivers SSCOPMCE PDU payload fragments for delivery to the user of the SSCOPMCE entity and accepts SSCOPMCE PDUs for transfer to the peer user. ~~Annex C describes the mapping of primitives across this SAP with IP and UDP.~~ Annexes C and D describe the mapping of primitives across this SAP with IP and UDP; Annex C covers legacy IP networks while Annex D covers IP networks that support differentiated services. Annex E covers operation over an Ethernet databus.

…

4) Clause 7.3.3

Modify as follows:

7.3.3 Connectionless environment

The signals defined in this subclause were originally defined for the ATM adaptation layer environment; they bear little resemblance to any known connectionless environment. For such environments a convergence function is needed (this is to a large extent a modelling artifact). Such ~~a~~ functions for IP or UDP based communications ~~is~~are defined in Annexes C and D ~~to this recommendation~~.

5) Clause C.1

Modify as follows:

C.1 General description

The convergence function for SSCOPMCE above IP provides for the possibility to deploy SSCOPMCE on top of the connectionless service provided by IP. The IP service utilises protocol defined in IETF RFCs 791 [8] and 1122 [10]. Alternatively, UDP service, as defined in IETF RFC 768 [7], may be used. Both alternatives are discussed in this annex.

All protocol stacks that include SSCOPMCE can, therefore, also be used in an IP-based networks. A particular application of this arrangement is a protocol stack for SS No. 7 signalling.

NOTE – The convergence function of this annex, being based upon IETF RFC 791 [8], is designed specifically for operation with IPv4. If use is desired of an application, e.g. the "Differentiated Services" defined in IETF RFC 2475 [19], which ~~IETF defined "DIFFSERV", that~~ is not compatible with IETF RFC 791 [8], then this annex is not applicable~~; for the application of "Differentiated Services" see Annex D.~~; for the application of "Differentiated Services" see Annex D.

6) Annexes D and E

Add new Annexes D and E:

ANNEX D

Convergence function for SSCOPMCE above IP or UDP with Differentiated Services

D.1 General description

The convergence function for SSCOPMCE above IP provides for the possibility to deploy SSCOPMCE on top of the connectionless service provided by IP. The IP service utilizes protocol defined in IETF RFCs 791 [8] and 1122 [10]. In addition, the Differentiated Services Field is defined in IETF RFC 2474 [10 *bis*]. Alternatively, UDP service, as defined in IETF RFC 768 [7], may be used. Both alternatives are discussed in this annex.

NOTE – The architecture of the differentiated service is described in IETF RFC 2475 [19].

All protocol stacks that include SSCOPMCE can, therefore, also be used in IP-based networks that deploy the differentiated service. A particular application of this arrangement is a protocol stack for SS No. 7 signalling.

D.2 Functions of the convergence function

The purpose of the convergence function is to map information between SSCOPMCE and IP (or UDP) PDUs. Appropriate headers must be created as is customarily done in the IP (or UDP) environment.

D.3 Specification of the convergence function

Clause 7.3 defines the primitives and parameters used at the lower boundary of the SSCOPMCE protocol entity. It shows that the parameters of the CPCS-UNITDATA.invoke primitive are used to model the transfer of information from SSCOPMCE protocol entity to the entity serving it. It also shows that the parameters of the CPCS-UNITDATA.signal primitive are used to model the transfer of information from the entity serving the SSCOPMCE protocol entity to that SSCOPMCE protocol entity.

D.3.1 The IP interface to its users

D.3.1.1 Description of the IP upper interface

The user interface to the IP is described by example in IETF RFC 791 [8] in a quasi-formal way through the exchange of "SEND" and "RECEIVE" primitives (although the language is modelled on descriptions of function calls in an operating system). All IP implementations must provide a certain minimum set of services to guarantee that all IP implementations can support the same protocol hierarchy.

Since Internet protocol is a datagram protocol, there is minimal memory or state maintained between datagram transmissions, and each call on the Internet protocol module by the user supplies all information necessary for the IP to perform the service requested.

When the user sends a datagram, it transmits the SEND primitive, supplying all the arguments. The Internet protocol module, on receiving this primitive, checks the arguments and prepares and sends the message. If either the arguments are bad, or the network does not accept the datagram, a reasonable report must be made to the user as to the cause of the problem, but the details of such reports are up to individual implementations.

When a datagram arrives at the Internet protocol module from the network, the information contained in the datagram is passed from the datagram to the user. If the user addressed does not exist, an ICMP error message is returned to the sender and the data is discarded, as described in IETF RFCs 792 [9] and 1122 [10].

IETF RFC 791 [8] defines the contents of the IP packet header as shown in Figure D.1.

<table>
<tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>3</td><td></td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td></tr>
<tr><td colspan="4">Version</td><td colspan="4">IHL</td><td colspan="8">Type of Service</td><td colspan="16">Total length</td></tr>
<tr><td colspan="16">Identification</td><td colspan="3">Flags</td><td colspan="13">Fragment Offset</td></tr>
<tr><td colspan="8">Time to Live</td><td colspan="8">Protocol</td><td colspan="16">Header Checksum</td></tr>
<tr><td colspan="32">Source Address</td></tr>
<tr><td colspan="32">Destination Address</td></tr>
<tr><td colspan="24">Options</td><td colspan="8">Padding</td></tr>
</table>

Figure D.1/Q.2111 – Example Internet Datagram Header

The fields of the header shown in Figure D.1 are defined in RFC 791 [8] as follows:

Version (4 bits)

The Version field indicates the format of the Internet header.

IHL (4 bits)

Internet Header Length is the length of the Internet header in 32 bit words, and thus points to the beginning of the data. Note that the minimum value for a correct header is 5.

Type of Service (8 bits)

When IPv4 is deployed on a network supporting the differentiated services, this field is used as the differentiated services field (DS field) as defined in IETF RFC 2474 [10 *bis*]. The DS field structure is defined as follows:

<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr>
<tr><td colspan="6">DSCP</td><td colspan="2">CU</td></tr>
</table>

DSCP: Differentiated Services Codepoint

Six bits of the DS field are used as a codepoint (DSCP) to select the per-hop behaviour a packet experiences at each node.

CU: Currently Unused

A two-bit currently unused (CU) field is reserved and its definition and interpretation are outside the scope of this Recommendation. The value of the CU bits are ignored by differentiated services-compliant nodes when determining the per-hop behaviour to apply to a received packet.

A specification of the packet forwarding treatments selected by the DS field values of "xxx000|xx", or DSCP = "xxx000" and CU subfield unspecified, are reserved as a set of Class Selector Codepoints. per-hop behaviours which are mapped to by these codepoints MUST satisfy the Class Selector per-hop behaviour requirements in addition to preserving the default per-hop behaviour requirement on codepoint "000000". In IETF RFC 2474 [10 *bis*], the meaning of the "Class Selector Codepoint" is defined as follows:

To preserve partial backwards compatibility with known current uses of the IP Precedence field without sacrificing future flexibility, we have taken the approach of describing minimum requirements on a set of per-hop behaviours that are compatible with most of the deployed forwarding treatments selected by the IP Precedence field. In addition, we give a set of codepoints that MUST map to per-hop behaviours meeting these minimum requirements. The per-hop behaviours mapped to by these codepoints MAY have a more detailed list of specifications in addition to the required ones stated here. Other codepoints MAY map to these same per-hop behaviours. We refer to this set of codepoints as the Class Selector Codepoints, and the minimum requirements for per-hop behaviours that these codepoints may map to are called the Class Selector per-hop behaviour Requirements.

The Precedence Field is defined in IETF RFC 791 [8] as follows:

Precedence

111	Network Control
110	Internetwork Control
101	CRITIC/ECP
100	Flash Override
011	Flash
010	Immediate
001	Priority
000	Routine

Total Length (16 bits)

Total Length is the length of the datagram, measured in octets, including Internet header and data. This field allows the length of a datagram to be up to 65 535 octets.

NOTE – The maximal Internet header is 60 octets, and a typical Internet header is 20 octets.

Identification (16 bits)

An identifying value assigned by the sender to aid in assembling the fragments of a datagram.

Flags (3 bits)

Various Control Flags.

Bit 0	reserved, must be zero
Bit 1 (DF)	0 = May Fragment, 1 = Don't Fragment.
Bit 2 (MF)	0 = Last Fragment, 1 = More Fragments.

Fragment Offset (13 bits)

This field indicates where in the datagram this fragment belongs. The fragment offset is measured in units of 8 octets (64 bits). The first fragment has offset zero.

Time to Live (8 bits)

This field indicates the maximum time the datagram is allowed to remain in the Internet system. If this field contains the value zero, then the datagram must be destroyed by an intermediate host (but not by the destination host). This field is modified in Internet header processing. The time is measured in units of seconds, but since every module that processes a datagram must decrease the TTL by at least one, even if it processes the datagram in less than a second, the TTL must be thought of only as an upper bound on the time a datagram may exist. The intention is to cause undeliverable datagrams to be discarded, and to bound the maximum datagram lifetime.

Protocol (8 bits)

This field indicates the next level protocol used in the data portion of the Internet datagram. The values for various protocols are specified by the IETF. The numeric value for SSCOPMCE is "128".

Header Checksum (16 bits)

A checksum on the header only. Since some header fields change (e.g. time to live), this is recomputed and verified at each point that the Internet header is processed.

The checksum field is the 16 bit one's complement of the one's complement sum of all 16 bit words in the header. For purposes of computing the checksum, the value of the checksum field is zero.

Source Address (32 bits)

The source address. See 3.2/IETF RFC 791 [8].

Destination Address (32 bits)

The destination address. See 3.2/IETF RFC 791 [8].

Options (variable)

The options may appear or not in datagrams. They must be implemented by all IP modules (host and gateways). What is optional is their transmission in any particular datagram, not their implementation.

In some environments the security option may be required in all datagrams.

The option field is variable in length. There may be zero or more options. The specific coding of the options field may be found in IETF RFC 791 [8].

D.3.1.2 Transmitter Side Mapping

Figure D.2 shows the Service Data Unit and Parameters passed between the SSCOPMCE/Convergence Function and the IP layer at the transmitting side. In this figure, it can be seen that the relevant fields of the IP packet header should be coded as shown in Table D.1.

D.3.1.3 Receiver Side Mapping

Figure D.3 shows the Service Data Unit and Parameters passed between SSCOPMCE/Convergence Function and the IP layer at the receiving side.

Table D.1/Q.2111 – Transmitter side mapping

Version	(Note 1)	
Internet Header Length (IHL)	(Note 1)	
Differentiated Services Field (Note 5)	00000000	If "Cell Loss Priority" = 1
	(Note 6)	If "Cell Loss Priority" = 0
Total Length (TL)	(Note 1)	
Identification	(Note 2)	
Flags	000	May fragment; last fragment
	001	May fragment; more fragments
Fragment Offset	(Note 1)	
Time to Live (TTL)	(Note 2)	
Protocol (PROT)	(Note 2)	"128"
IP Header Checksum	(Note 1)	
Source Address	(Note 2)	the IP address of the source node
Destination Address	(Note 2)	the IP address of the destination node
Options	(Note 1)	(Note 4)
Data	(Note 3)	1 to (65 535 – IHL)

NOTE 1 – Coding of this parameter is handled by the IP module using guidance provided in IETF RFC 791 [8].

NOTE 2 – Coding of this parameter is handled by the convergence function using the rules specified in IETF RFC 791 [8].

NOTE 3 – The SSCOP-PDU is appended with the CPCS-PDU trailer, coded as specified in ITU-T I.363.5 [5].

NOTE 4 – For the purpose of this Recommendation, the user options "Loose Source and Record Route," "Strict Source and Record Route," "Record Route," and "Timestamp~~Timeshare~~" apply. Other user options shall not be used and shall be silently ignored when received (see IETF RFC 1122 [10] section 3.2.1.8). It should be noted that the options "No Operation" (Type 1) and "End of List" (Type 0) are to be handled within the IP module; therefore, they are not passed to the transport layer.

NOTE 5 – A replacement header field, called the DS field, is defined, which is intended to supersede the existing definitions of the IPv4 TOS octet (see RFC 791 [8]).

NOTE 6 – This field should be set to a value representing the quality equal to "Cell Loss Priority = 0". Therefore, the first three bits should be greater than "000", e.g. "11100000" in a network where it is appropriate.

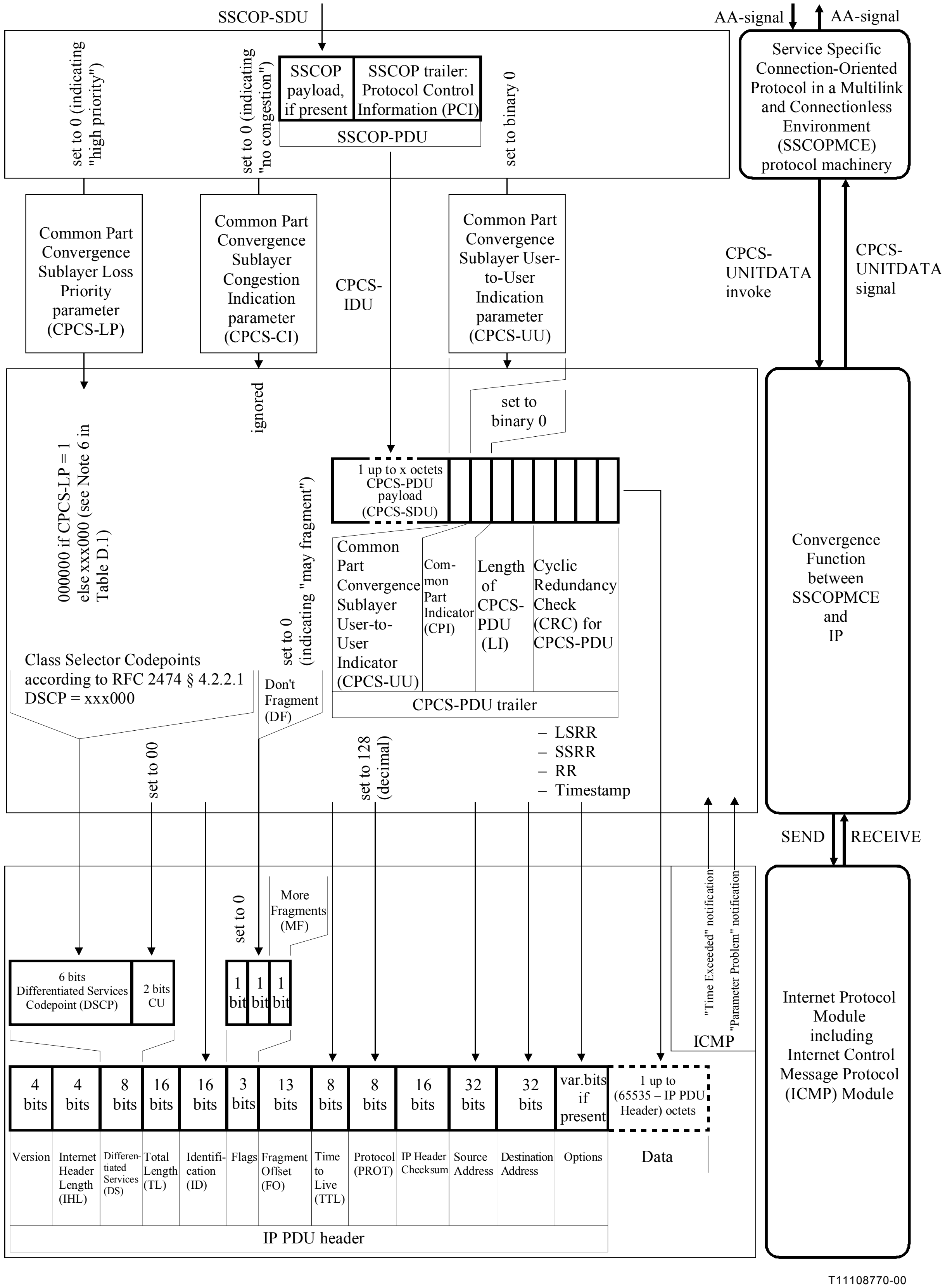

Figure D.2/Q.2111 – Service Data Unit and Parameters passed between SSCOPMCE/Convergence Function and IP Layer – Transmitting side

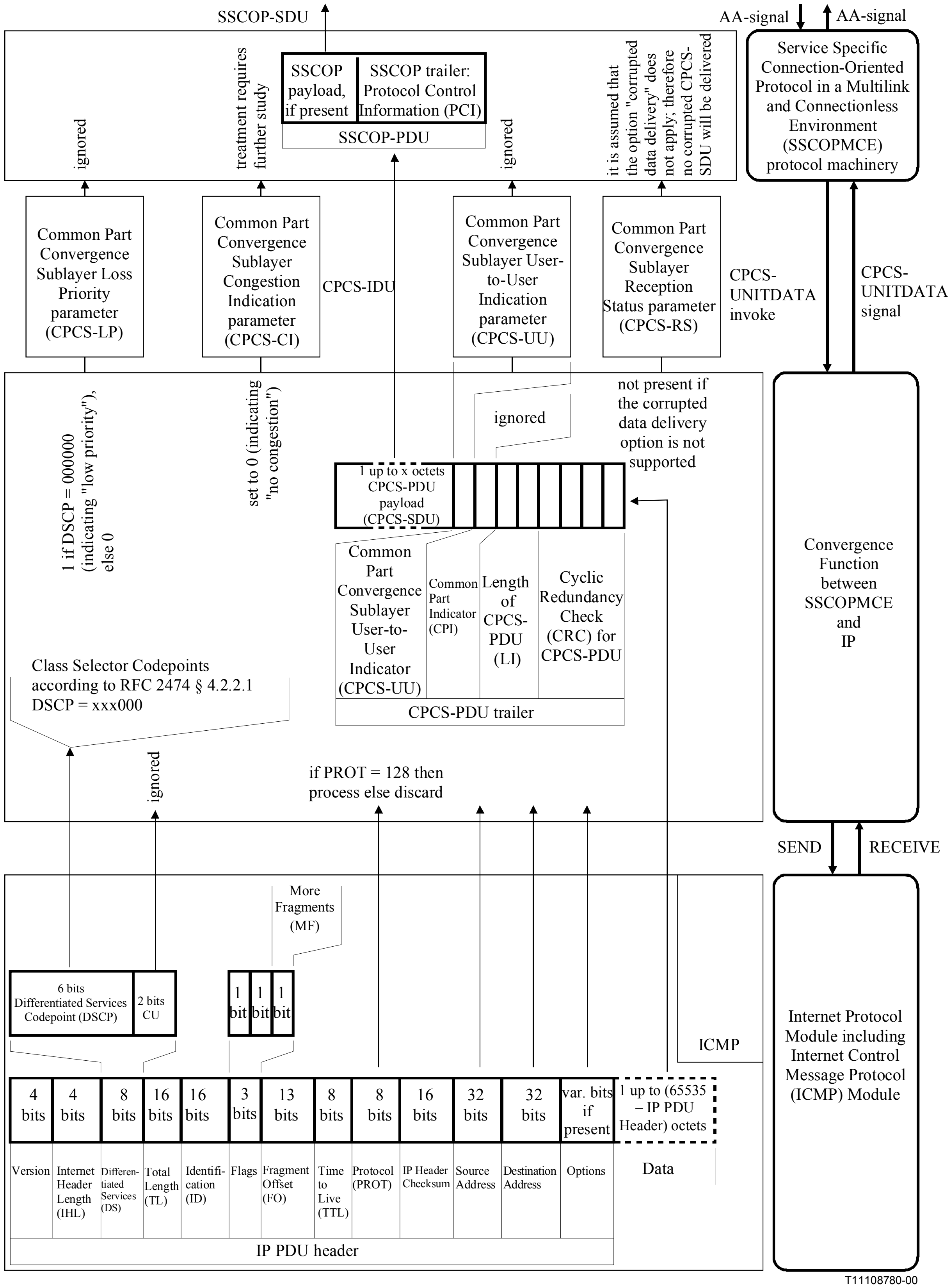

Figure D.3/Q.2111 – Service Data Unit and Parameters passed between SSCOPMCE/Convergence Function and IP Layer – Receiving side

D.3.2 The UDP interface to its users

D.3.2.1 Description of the UDP upper interface

IETF RFC 768 [7] defines the parameters of the UDP packet header as shown in Figure D.4.

0 7 8 15	16 23 24 31
Source Port	Destination Port
Length	Checksum
data octets ...	

Figure D.4/Q.2111 – UDP Header Format

The fields of the header shown in Figure D.4 are defined in RFC 768 [7] as follows:

Source Port (16 bits)

Source Port is an optional field, when meaningful, it indicates the port of the sending process, and may be assumed to be the port to which a reply should be addressed in the absence of any other information. If not used, a value of zero is inserted.

Destination Port (16 bits)

Destination Port has a meaning within the context of a particular Internet destination address.

Length (16 bits)

Length is the length in octets of this user datagram including this header and the data. (This means the minimum value of the length is eight.)

Checksum (16 bits)

Checksum is the 16-bit one's complement of the one's complement sum of a pseudo-header of information from the IP header, the UDP header, and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

The pseudo-header conceptually prefixed to the UDP header contains the source address, the destination address, the protocol, and the UDP length. This information gives protection against misrouted datagrams. This checksum procedure is the same as is used in TCP.

NOTE – For the purpose of this Recommendation the source address, the destination address, and the protocol are modelled as parameters.

D.3.2.2 Transmitter Side Mapping

Figure D.5 shows the Service Data Unit and Parameters passed between the SSCOPMCE/Convergence Function and the UDP and IP modules at the transmitting side.

D.3.2.3 Receiver Side Mapping

Figure D.6 shows the Service Data Unit and Parameters passed between the SSCOPMCE/Convergence Function and the UDP and IP modules at the receiving side.

D.4 Layer Management

There are no interactions with layer management defined.

It is for further study to determine whether a need exists for the Convergence Function to invoke the services of the Internet Control Message Protocol (ICMP) to notify the peer of error situations, such as Protocol Unreachable and Port Unreachable, in the absence of a peer-to-peer mechanism (see IETF RFC 1122 [10] section 3.2.2.1).

It is for further study to determine whether SSCOPMCE should provide positive and/or negative advice to modify the routing of messages upon "Dead Gateway Detection" (see IETF RFC 1122 [10] section 3.3.1.4).

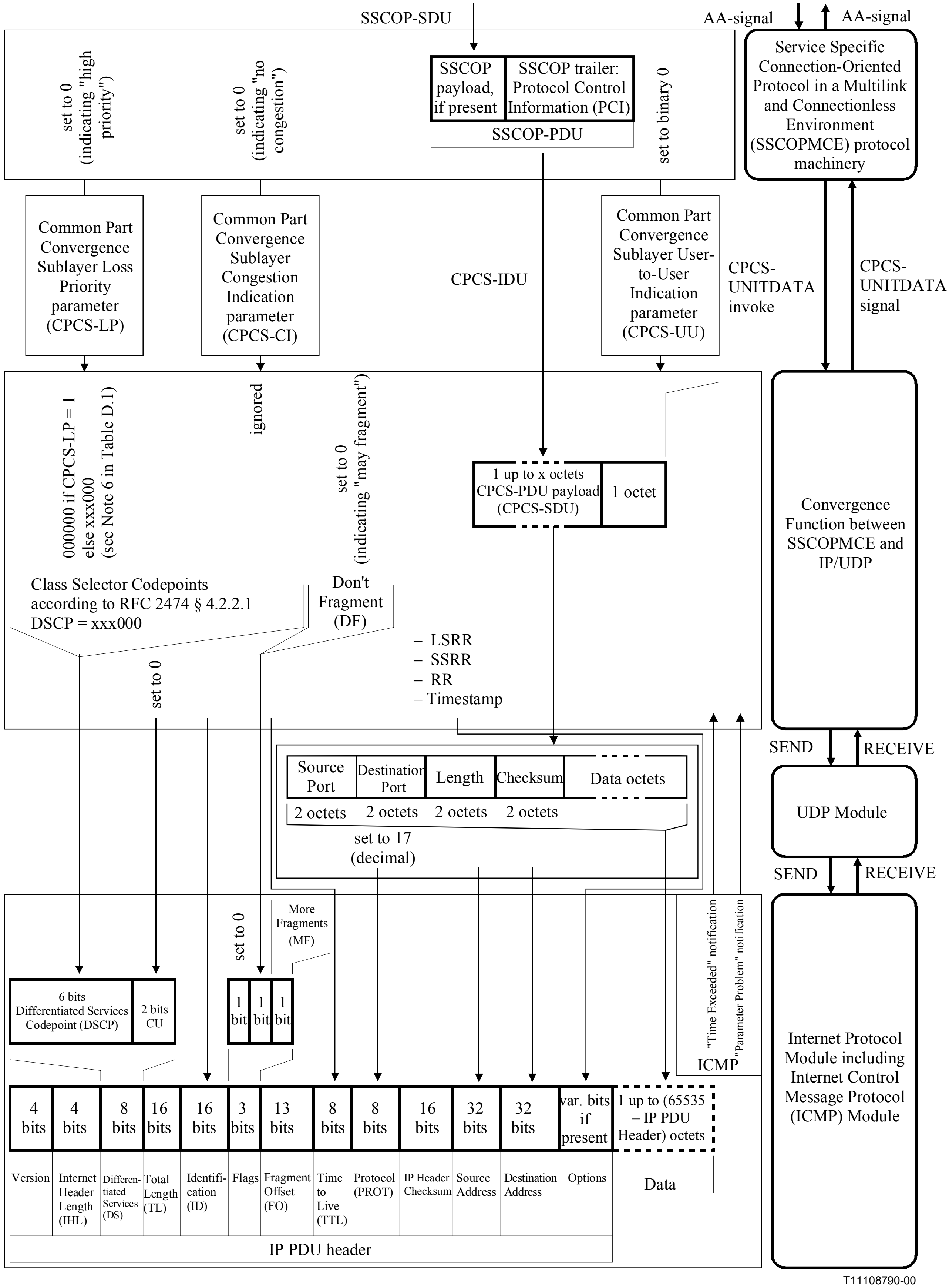

Figure D.5/Q.2111 – Service Data Unit and Parameters passed between SSCOPMCE/ Convergence Function and UDP/IP Layer – Transmitting side

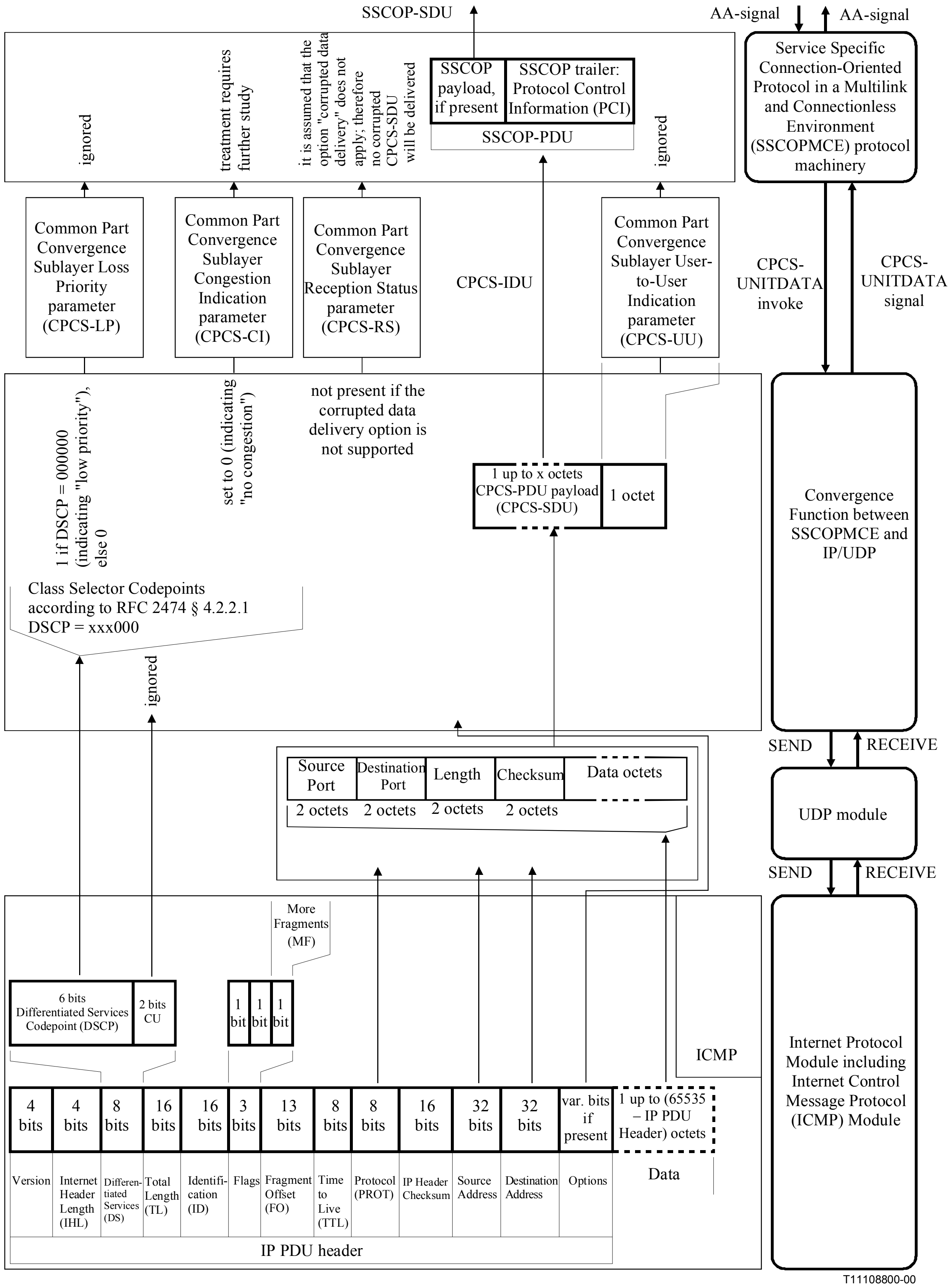

Figure D.6/Q.2111 – Service Data Unit and Parameters passed between SSCOPMCE/Convergence Function and UDP/IP Layer – Receiving side

ANNEX E

Convergence Function for SSCOPMCE Above Ethernet

E.1 General Description

The convergence function for SSCOPMCE above Ethernet specifies the deployment of SSCOPMCE on top of the connectionless service provided by IEEE 802.3 Ethernet networks according to ISO/IEC 8802-3 [10 *ter*][1]. A primary driver for this configuration is to realize an open-systems databus for closed-loop systems. A switched, full-duplex mode of operation is assumed, though not required, for operation of SSCOPMCE above an Ethernet-based infrastructure.

E.2 Functions of the Convergence Function

The purpose of the convergence function is to map information between SSCOPMCE and Ethernet PDUs.

E.3 Ethernet Interface

The user interface to an Ethernet MAC layer service is defined by the IEEE 802.3 tagged MAC frame format, as shown in Figure E.1. Figure E.1 is a replication of Figure 3-3 of ISO/IEC 8802-3 [10 *ter*][1]. Each frame represents the equivalent of an Ethernet PDU.

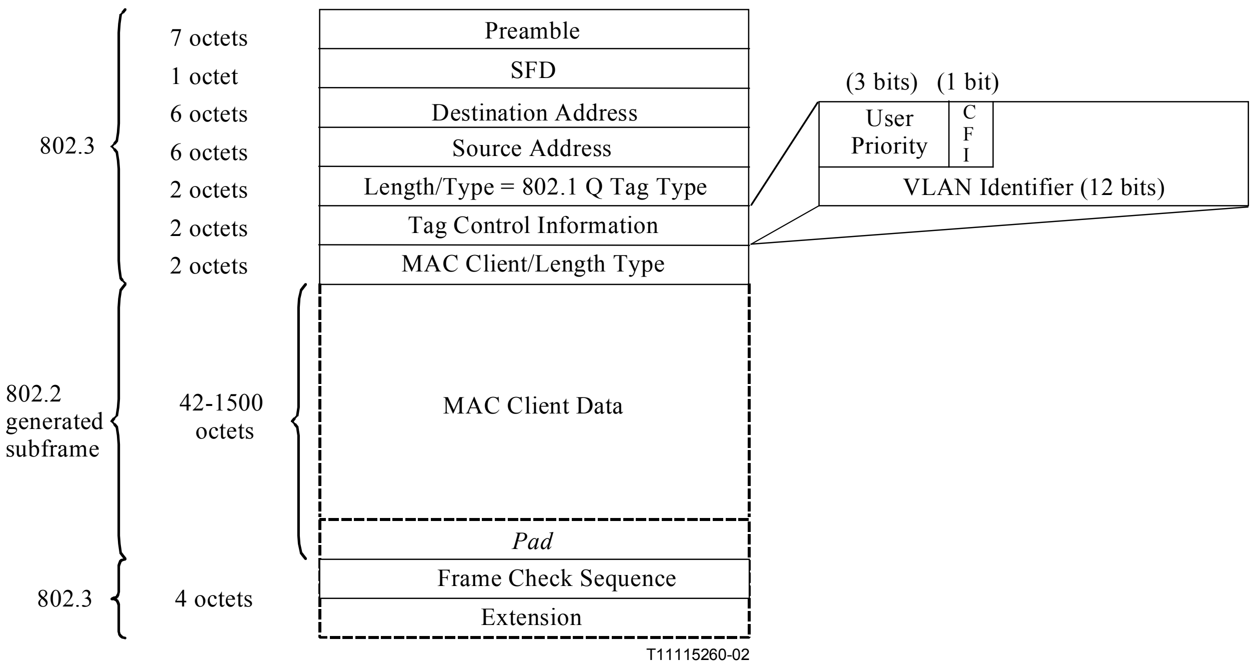

Figure E.1/Q.2111 – 802.3 tagged MAC frame format

The 802.3 tagged MAC frame has the following fields and shall take values as defined below:

E.3.1 Preamble Field

Preamble is a 7-octet field that is used to allow circuitry to reach synchronization with the received frame timing. The preamble pattern shall take the value:

10101010 10101010 10101010 10101010 10101010 10101010 10101010

in accordance with ISO/IEC 8802-3 clause 4.2.5 [10 *ter*].

---

[1] IEEE 802.3, 2000 Edition has been adopted by ISO/IEC and redesignated as ISO/IEC 8802-3:2000.

E.3.2 Start Frame Delimiter

The SFD field has shall take the value 10101011, in accordance with ISO/IEC 8802-3 clause 3.2.2 [10 *ter*]. It indicates the start of a frame.

E.3.3 Address Fields

A destination address field specifies the destination address for which the frame in intended. The Source address identifies the station from which the frame is initiated. In both cases, the address field is 6 octets (48 bits) long. The first bit in the address identifies the address an individual or group address. The second bit distinguished between locally or globally administered addresses. An all 1s in the destination address field is defined as the broadcast address to all stations on the communication medium.

E.3.4 Length/Type Field

A length/type field is 2 octets long. It shall take the value 0x8100 (hexadecimal), in accordance with ISO/IEC 8802-3 clause 3.5.4 [10 *ter*]. This indicates the existence of a tag field (and not an Sub-Network Access Protocol (SNAP) Identifier). Details are provided in IEEE 802.1Q, clauses 9.3 and 9.3.1 [22].

E.3.5 Tag Control Information

Tag control information (TCI) is 2 octets long and is subdivided into the following sub-fields:

- A 3-bit user priority field (Class of Service Parameter).
- A 1-bit Canonical Format Identifier (CFI).
- A 12-bit Virtual Local Area Network (VLAN) identifier (VID).

The priority sub-field enables differentiated treatment of frames based on their priority. According to ISO/IEC 15802-3 clauses 6.5.1 and 6.4 [21], the range of this parameter is in the range from 0 through 7. The default user priority value is 0. The values from 1 through 7 form an ordered sequence of user priorities, with 1 being the lowest priority and 7 the highest.

The CFI sub-field is a flag indicating whether or not the MAC address information present in the client data part of the MAC frame is in Canonical format.

According to IEEE 802.1Q clause 9.3.2.2 b) [22], when the tag header indicates "Ethernet-encoded", the CFI has the following meaning:

1) When set, indicates that the E-RIF field is present in the tag header, and that the NCFI bit in the RIF determines whether MAC Address information that may be present in the MAC data carried by the frame is in Canonical (C) or Non-canonical (N) format;
2) When reset, indicates that the E-RIF field is not present in the tag header, and that all MAC Address information that may be present in the MAC data carried by the frame is in Canonical (C) format.

For the purpose of Annex E, the CFI shall be reset, i.e. binary 0.

The VID sub-field provides explicit tagging of VLAN membership information in order to identify broadcast domains within a switched Ethernet network. According to IEEE 802.1Q clause 9.3.2.3 [22], the full range of VID values may be supported (0-4096); however the following VID values are reserved with specific meanings:

1) 0 (hexadecimal) is "null VLAN ID" (tag header contains only priority information)
2) 1 (hexadecimal) is "default Port Virtual LAN Identifier (PVID)" (for port-based VLAN classification of frames)
3) FFF (hexadecimal) is "reserved for implementation use" and shall not be:
   a) configured as PVID;

b) configured in any Filtering Database entry;

c) used in any Management operation; or

d) transmitted in a tag header.

NOTE – Details see IEEE 802.1Q Table 9-2 [22].

The priority and VLAN sub-fields denote the ISO/IEC 15802-3 [21] and IEEE 802.1Q [22] standards, respectively.

E.3.6 MAC Client Length/Type Field

The MAC Client Length/Type field as two interpretations, depending upon its value. For numeric evaluation, the first octet is the most significant octet of this field.

- When the value of this field is less than or equal to the value of `maxValidFrame` (see ISO/IEC 8802-3 clause 4.2.7.1 and for implementation-dependent values, clause 4.4 [10 *ter*]), then the field indicates the number of octets contained in the subsequent data field of the frame (Length interpretation).
- When the value of the field is greater than or equal to 1536 decimal (0x0600) the field indicates the nature of the MAC client protocol (Type interpretation). The Type value used to indicate SSCOPMCE as the client protocol is 8900 decimal (0x22C4).

This annex defines the SSCOPMCE mapping to IEEE-based (i.e. ISO/IEC 8802-3 [10 *ter*]) Ethernet networks only.

E.3.7 Logical Link Control, Data and Pad Fields

Logical Link Control (LLC) defines MAC-independent logical layer services to pass incoming frames to an appropriate network layer protocol (see ISO/IEC 8802-2 clause 2.2 [20]):

The 802.2 subframe generated by the LLC layer has traditionally contained a LLC header field and a data field. Since a minimum frame size is required for correct MAC-layer operation, the data field may be appended with extra bits, i.e. a pad field. Recently, use of the LLC header has been deprecated in practice and thus it is not to be used. Instead, alternate protocol fields (i.e. port identifiers described in E.5 providing an identical function in a simpler manner have been specified.

E.3.8 Frame Check Sequence Field

A cyclic redundancy check is used by the transmit and the receive algorithms to generate a CRC value for the FCS field. The FCS field contains a 4-octet CRC value and is defined in ISO/IEC 8802-3 clause 3.2.8 [10 *ter*].

E.3.9 Extension Field

The Extension field contains a sequence of extension bits. Its length may be zero to (`slotTime – minFrameSize`) bits (see ISO/IEC 8802-3 clause 4.2.7.1 and for implementation-dependent values, clause 4.4 [10 *ter*]). The contents of the Extension field are not included in the FCS computation.

E.4 Mappings

Mappings between SSCOPMCE and Ethernet are shown in Figures E.2 and E.3, which depict the service data units and parameters passed between the SSCOPMCE/Convergence Function and the Ethernet layer at the transmitting and receiving side, respectively.

E.5 Upper Layer Service Access

The SSCF sublayer provides the SAP to applications that utilize SSCOPMCE services. (That SAP is in contrast to the SAP between the convergence function and datalink layer, defined in E.3.) The mapping between the SSCF and SSCOP sublayers is the same as that defined for the Service Specific Coordination Function for Support of Signalling at the User Network Interface (SSCF at

UNI) specified in ITU-T Q.2130 [12]. As a result, applications will be able to utilize the SAP to access the following services enabled by SSCOPMCE:

- Unacknowledged transfer of data;
- Assured transfer of data;
- Transparency of transferred information;
- Establishment and release of connections for assured transfer of data.

The SSCF SAP, as well as a SAP to Ethernet MAC-layer elements, together form an access to user-network interface that supports SSCOPMCE above Ethernet. For the purpose of this annex, the only unique requirement on that access is that it supports the specification of port information. Within the SSCOPMCE protocol machinery and convergence function, this means that four octets will be aligned with each SSCOP SDU, to be located in the MAC client data field before the CPCS-PDU (that is also contained in the MAC client data field together with padding, if required); two octets representing a source port, and two octets representing a destination port. These identifiers will be used to multiplex/demultiplex SSCOPMCE sessions across multiple application processes; the processes would be utilizing a common Ethernet interface. (The port identifier can be thought of as reusing a subset of the space traditionally occupied by the five-octet SNAP field, which followed the LLC field, but is rarely used on ISO/IEC 8802-3 networks.) Whether or not the SSCOP SDU is segmented by the convergence function to conform to the Ethernet maximum transmission unit, the port identifiers must be replicated in each Ethernet PDU on the transmitting side (Figure E.2), and extracted and aligned with a complete SSCOP SDU on the receiving side (Figure E.3).

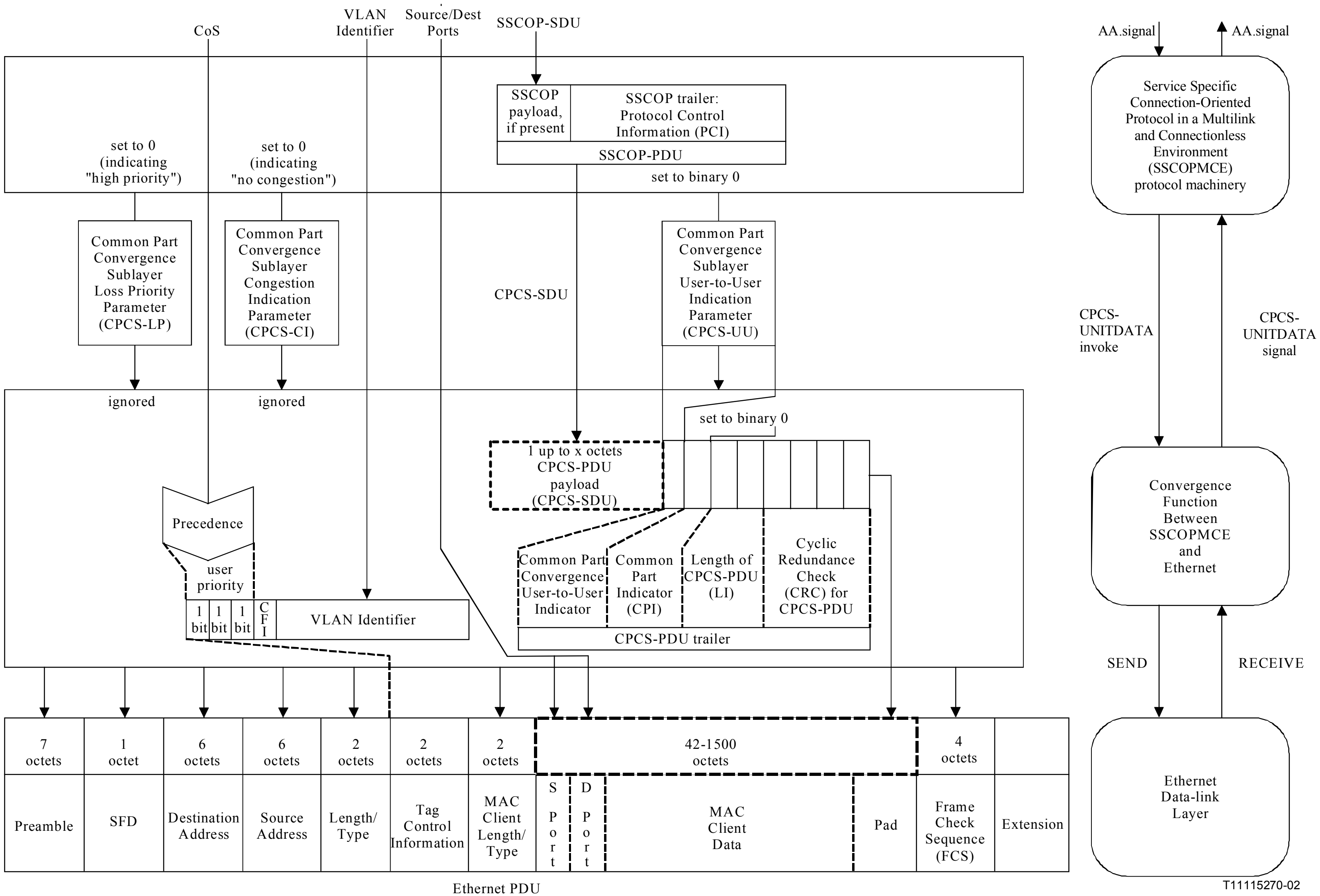

Figure E.2/Q.2111 – Service Data Unit and Parameters Passed Between SSCOP/Convergence Function and Ethernet – Transmitting Side

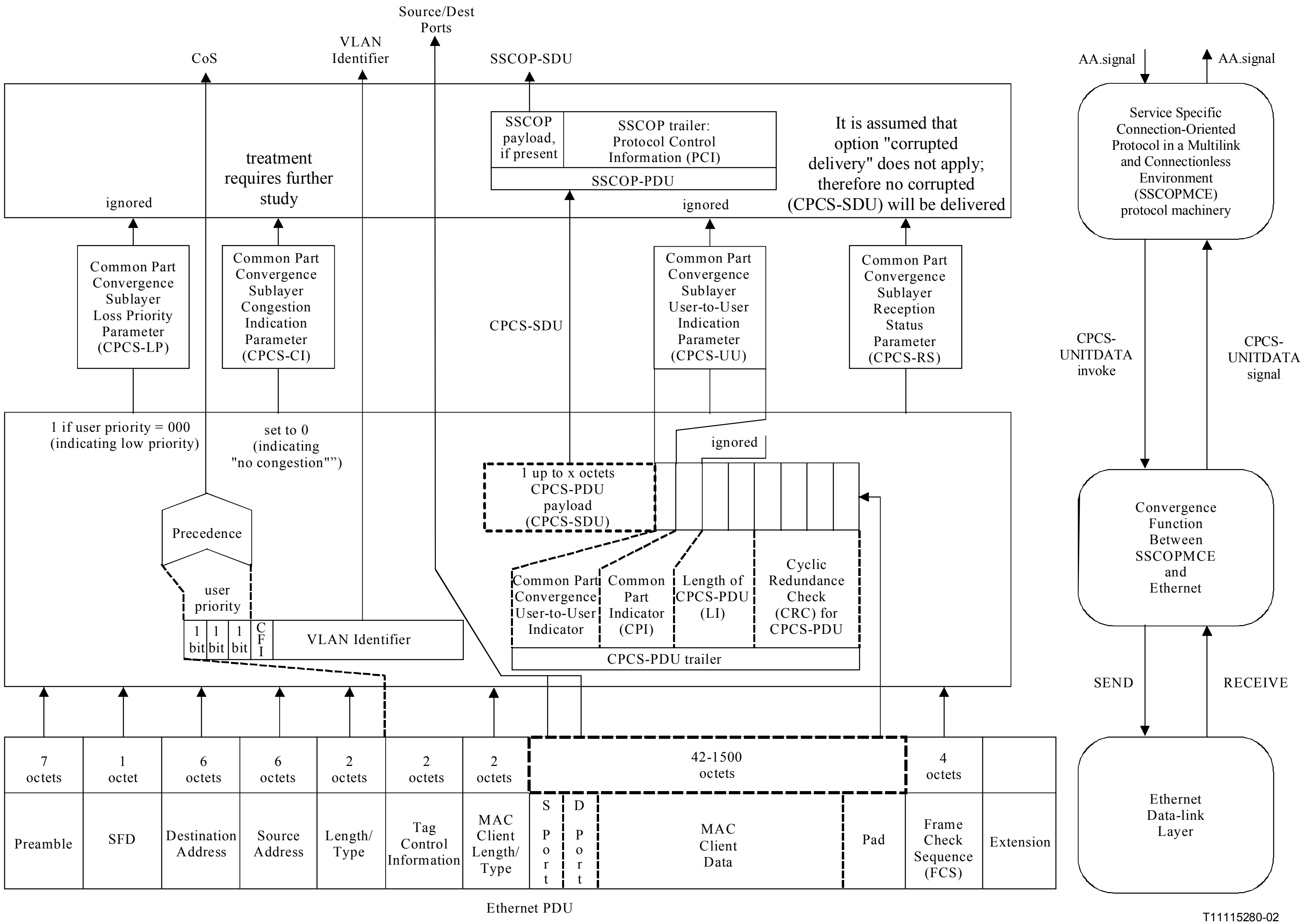

Figure E.3/Q.2111 – Service Data Unit and Parameters Passed Between SSCOP/Convergence Function and Ethernet – Receiving Side

7) Appendix I

Replace Appendix I with the following:

APPENDIX I[2]

Protocol Implementation Conformance Statement (PICS) Proforma

I.1 Introduction

`DH0:` Prior to the conformance testing and the interoperability testing of Implementations Under Test (IUTs), it is necessary to have the PICS (Protocol Implementation Conformance Statement) document for an implementation.

`DH1:` This particular PICS deals with the implementation of the Service Specific Connection Oriented Protocol in a Multilink and Connectionless Environment (SSCOPMCE).

I.1.1 Scope

`DH2:` This document provides the PICS proforma for the Service Specific Connection Oriented Protocol in a Multilink and Connectionless Environment (SSCOPMCE) [1], in compliance with the relevant requirements, and in accordance with the relevant guidelines, given in ITU-T X.296 [3].

I.1.2 Normative References

[1] ITU-T Q.2111 (1999), *Service specific connection oriented protocol in a multilink and connectionless environment (SSCOPMCE)*.

[2] ITU-T X.290 (1995), *OSI conformance testing methodology and framework for protocol Recommendations for ITU-T applications – General concepts*.

[3] ITU-T X.296 (1995), *OSI conformance testing methodology and framework for protocol Recommendations for ITU-T applications – Implementation conformance statements*.

I.1.3 Definitions

IUT Implementation Under Test

M Mandatory statement

N/A Not applicable

NOT item not supported; absence of item

O Optional

O.<n> Optional, but, if chosen, support is required for either at least one or only one of the options in the group labeled by the same numeral <n>

PDU Protocol Data Unit

PICS Protocol Implementation Conformance

S.<i> Supplementary information number i

SDU Service Data Unit

---

[2] **Copyright release for PICS proforma**

Users of this Recommendation may freely reproduce the PICS proforma in this appendix so that it can be used for its intended purpose, and may further publish the completed PICS.

SUT System Under Test

X.<i> Exceptional information number i

I.1.4 Conformance Statement

DH3: The supplier of a protocol implementation, which is claimed to conform to the Service Specific Connection Oriented Protocol in a Multilink and Connectionless Environment Specification (SSCOPMCE), is required to complete a copy of the PICS proforma provided in I.2 and is required to provide the information necessary to identify both the supplier and the implementation.

DH3a: NOTE – For the purpose of making such a statement, this Appendix may be copied without further permission.

I.2 PICS Proforma

I.2.1 Identification of the PICS Proforma Corrigenda

Identification of corrigenda applied to this PICS proforma	ITU-T Q.2111 (2000) Corr.: Corr.:

I.2.2 Instructions for Completing the PICS Proforma

DH4: The PICS Proforma is a fixed-format questionnaire. Answers to the questionnaire should be provided in the rightmost columns, either by simply indicating a restricted choice (such as Yes or No), or by entering a value or a set of range of values.

DH5: A supplier may also provide additional information, categorized as exceptional or supplementary information. An exception item should contain the appropriate rational.

DH6: The supplementary information is not mandatory and the PICS is complete without such information. The presence of optional supplementary or exception information should not affect test execution, and will in no way affect interoperability verification.

DH7: NOTE – Where an implementation is capable of being configured in more than one way, a single PICS may be able to describe all such configurations. However, the supplier has the choice of providing more than one PICS, each covering some subset of the implementation's configuration capabilities, in case this makes for easier or clearer presentation of the information.

I.2.3 Identification of the Implementation

Implementation Under Test (IUT)

<u>Identification</u>

IUT Name: ______________________________

IUT Version: ______________________________

____

<u>System Under Test</u>

SUT Name: ______________________________

____

Hardware Configuration: ______________________________

____

____

Operating System: ______________________________

<u>Product Supplier</u>

Name: ______________________________

Address: ______________________________

____

Telephone Number: ______________________________

Facsimile Number: ______________________________

Email Address (optional): ______________________________

Additional Information: ______________________________

<u>Client</u>

Name: ______________________________

Address: ______________________________

____

Telephone Number: ______________________________

Facsimile Number: ______________________________

Email Address (optional): ______________________________

Additional Information: ______________________________

<u>PICS Contact Person</u>

Name: ______________________________

Address: ______________________________

____

Telephone Number: ______________________________

Facsimile Number: ______________________________

Email Address (optional): ______________________________

Additional Information: ______________________________

Identification of the protocol

DI0: This PICS proforma applies to the following document:

ITU-T Q.2111, *Service specific connection oriented protocol in a multilink and connectionless environment (SSCOPMCE).*

I.2.4 Global Statement of Conformance

DI1: The implementation described in this PICS meets all of the mandatory requirements of the reference protocol.

___Yes

___No

DI2: NOTE – Answering "No" indicates non-conformance to the specified protocol. Non-supported mandatory capabilities are to be identified in the PICS, with an explanation of why the implementation is non-conforming.

I.2.4.1 Roles

Item number	Item description	Ref.	Status	Support
R1	Transmitter and Receiver as a general protocol engine	5.1	O.1	
R2	Transmitter and Receiver in a restricted protocol engine	5.1	O.1	
O.1	Support of one and only one of these items is required			

I.2.4.2 Major capabilities

Item number	Item description	Ref.	Status	Support
MC1	Multilink mode (Mode "A")	5.3; 6 k); 8.7 a)	O.1	
MC2	Connectionless mode (Mode "B")	5.3; 6 k); 8.7 a)	O.1	
MC3	Compatibility mode (to Q.2110 procedures – Mode "C")	5.3; 6 k); 8.7 a)	O.1	
MC4	Assured data transfer between two SSCOPMCE users	5.2; 6 h)	R1 M R2 O	
MC5	Unassured data transfer between two SSCOPMCE users	5.2; 6 h)	R1 M R2 O	
MC6	Unassured data transfer between two SSCOPMCE layer management entities	5.2; 6 h)	R1 M R2 O	
MC7	Connection establishment, release, and resynchronization	5.2; 6 g)	R1 or MC4 M R2 O	
MC8	Out-of-sequence delivery	5.2; 6 l)	R1 M R2 and MC4 O R2 and not MC4 N/A	

Item number	Item description	Ref.	Status	Support
MC9	Local data retrieval by the user	5.2; 6 f)	R1 M R2 and MC4 O R2 and not MC4 N/A	
MC10	Error reporting to layer management	5.2; 6 d)	R1 M R2 and MC4 O R2 and not MC4 N/A	
MC11	Adding and removing links	5.4; 7.2.1 d) e)	M	
O.1	Support of at least one of these items is required			

I.2.4.3 SSCOPMCE protocol functions

Item number	Protocol function	Ref.	Status	Support
PF1	Assured data transfer with sequence integrity	6 a) h); 7.1.1 c); 8.1 j)	MC4 M not MC4 N/A	
PF2	Assured data transfer with error correction by selective retransmission	6 b) h); 7.1.1 c); 8.1 j)	MC4 M not MC4 N/A	
PF3	Assured data transfer with flow control	6 c) h); 7.1.1 c); 8.1 j)	MC4 M not MC4 N/A	
PF4	Keep alive function	6 e)	MC4 M not MC4 N/A	
PF5	Connection establishment for the management of assured data transfer	6 g); 7.1.1 a); 8.1 a) b) c)	MC4 M not MC4 N/A	
PF6	Connection release for the management of assured data transfer	6 g); 7.1.1 b); 8.1 d) e)	MC4 M not MC4 N/A	
PF7	Connection resynchronization for the management of assured data transfer	6 g); 7.1.1 d); 8.1 f) g)	MC4 M not MC4 N/A	
PF8	Protocol error detection and recovery	6 i); 7.1.1 e); 8.1 h) i)	MC4 M not MC4 N/A	
PF9	Status reporting	6 j); 8.1 k) l) m)	MC4 M not MC4 N/A	
PF10	Error reporting to layer management	6 d); 7.2.1 a)	MC4 and MC10 M else N/A	
PF11	Local data retrieval	6 f); 7.1.1 g) h)	MC4 and MC9 M else N/A	
PF12	Out of sequence delivery	6.1 h); 7.1.1 c); 8.1 j)	MC4 and MC8 M else N/A	

Item number	Protocol function	Ref.	Status	Support
PF13	Unassured data transfer betwen users	6 h); 7.1.1 f); 8.1 n)	MC5 M not MC5 N/A	
PF14	Transfer of Management-Data	6 m); 7.2.1 b); 8.1 o)	MC6 M not MC6 N/A	

I.2.4.4 PDUs

Item number	Item description	Ref.	Status	Support
PDU type				
PDU1 (Note)	BGN PDU	8.1 a); Figure 5	MC4 M not MC4 N/A	
PDU2 (Note)	BGAK PDU	8.1 b); Figure 6	MC4 M not MC4 N/A	
PDU3 (Note)	BGREJ PDU	8.1 c); Figure 7	MC4 M not MC4 N/A	
PDU4 (Note)	END PDU	8.1 d); Figure 8	MC4 M not MC4 N/A	
PDU5 (Note)	ENDAK PDU	8.1 e); Figure 9	MC4 M not MC4 N/A	
PDU6 (Note)	RS PDU	8.1 f); Figure 10	MC4 M not MC4 N/A	
PDU7 (Note)	RSAK PDU	8.1 g); Figure 11	MC4 M not MC4 N/A	
PDU8 (Note)	ER PDU	8.1 h); Figure 12	MC4 M not MC4 N/A	
PDU9 (Note)	ERAK PDU	8.1 i); Figure 13	MC4 M not MC4 N/A	
PDU10 (Note)	SD PDU	8.1 j); Figure 14	MC4 M not MC4 N/A	
PDU11 (Note)	POLL PDU	8.1 k); Figure 15	MC4 M not MC4 N/A	
PDU12 (Note)	STAT PDU	8.1 l); Figure 16	MC4 M not MC4 N/A	
PDU13 (Note)	USTAT PDU	8.1 m); Figure 7	MC4 M not MC4 N/A	
PDU14 (Note)	UD PDU	8.1 n); Figure 18	MC5 M not MC5 N/A	
PDU15 (Note)	MD PDU	8.1 o); Figure 18	MC6 M not MC6 N/A	
PDU16	Invalid PDU recognition and discard	8.1	M	

Item number	Item description	Ref.	Status	Support
	Formats			
PDU17	Coding conventions	8.2.1	M	
PDU18	Padding in SD PDUs and use of PL field	8.2.2 a)	MC4 M not MC4 N/A	
PDU19	Padding in UD PDUs and use of PL field	8.2.2 a)	MC5 M not MC5 N/A	
PDU20	Padding in MD PDUs and use of PL field	8.2.2 a)	MC6 M not MC6 N/A	
PDU21	Padding in BGN, BGAK, BGREJ, END, and RS PDUs and use of PL field	8.2.2 b)	MC4 M not MC4 N/A	
PDU22	Padding in STAT and USTAT PDUs	8.2.2 c)	MC4 M not MC4 N/A	
PDU23	Reserved fields	8.2.3	M	
PDU24	PDU Length	8.2.4	M	
PDU25	Coding of the list elements in STAT and USTAT PDUs	8.2.5	MC4 M not MC4 N/A	
PDU26	Segmentation of STAT PDUs	8.2.5	MC4 M not MC4 N/A	
NOTE – The coding of the fields of the PDUs is specified in clause 8.5.				

I.2.4.5 Arithmetic operations on state variables

This clause is applicable only if the major capability MC4 is implemented.

Item number	Item description	Ref.	Status	Support
	Modulo arithmetic			
AO1	Modulo 2^{24} arithmetic of state variables VT(S), VT(A), VT(MS), VT(H), VR(R), VR(H), VR(MR), and VR(S)	8.4.1	M	
AO2	Modulo 2^{24} arithmetic of state variables VT(PS), VT(PA), VR(PS), and VR(SPS)	8.4.1	M	
AO3	Modulo 2^{8} arithmetic of state variables VT(SQ) and VR(SQ)	8.4.1	M	
	Base for comparison			
AO4	VT(A) – 2^{23} when involving SD PDU sequemce numbers at the transmitter	8.4.1	M	
AO5	VR(R) – 2^{23} when involving SD PDU sequemce numbers at the receiver	8.4.1	M	
AO6	VT(PA) – 2^{23} when involving POLL PDU sequemce numbers at the transmitter	8.4.1	M	
AO7	VR(PS) – 2^{233} when involving POLL PDU sequemce numbers at the receiver	8.4.1	M	
AO8	VR(SQ) – 2^{7} when involving N(SQ) of SD PDUs	8.4.1	M	

I.2.4.6 Value range of state variables

This clause is applicable only if the major capability MC4 is implemented.

Item number	Item description	Ref.	Status	Support
VR1	Value range for VT(PD) of "0" to the maximum permissible value of "MaxPD"	I.2.5.1	M	
VR2	Value range for VT(CC) of "0" to the maximum permissible value of "MaxCC"	I.2.5.1	M	
VR3	Value range for VT(SS) of "0" to "255"	8.4.1	M	
VR4	Value range for VR(SS) of "0" to "255"	8.4.1	M	
VR5	Size of the boolean array of VT(x) at least the maximum permissible value of "MaxLinks"	8.4.1	M	
VR6	Size of the boolean array of VR(x) at least the maximum permissible value of "MaxLinks"	8.4.1	M	
VR7	Value range for nlinks of "0" to the maximum permissible value of "MaxLinks"	8.4.1	M	

I.2.4.7 Protocol features

This clause is applicable only if the major capability MC4 is implemented.

NOTE – The protocol features refer to the SDL diagrams; any implementation showing to the environment the same behavior as the SDL diagrams is conforming.

I.2.4.7.1 Start-up

Item number	Protocol Feature	Ref.	Status	Support
PSU1	State "Guard" and Timer_GUARD	Figure 22 (2 of 38)	M	
PSU2	Initialization of state variables	Figure 22 (2 of 38)	M	

I.2.4.7.2 Connection control procedures

Item number	Protocol Feature	Ref.	Status	Support
PCC1	Connection establishment and release	Figure 22 (3 to 10 of 38)	M	
PCC2	Connection resynchronization	Figure 22 (11 to 15 of 38)	MC4 and PF7 M else N/A (Note 1)	
PCC3	Connection recovery	Figure 22 (16 to 21 of 38)	MC4 and PF8 M else N/A (Note 2)	
PCC4	Active Timer_CC in states 2, and 4	Figure 22 (5 and 9 of 38)	M	

Item number	Protocol Feature	Ref.	Status	Support
PCC5	Active Timer_CC in state 5	Figure 22 (11 of 38)	MC4 and PF7 M else N/A	
PCC6	Active Timer_CC in state 7	Figure 22 (16 of 38)	MC4 and PF8 M else N/A	
PCC7	Exiting state 10 "Data Transfer Ready"	Figure 22 (22 to 24 of 38)	M	
NOTE 1 – If States 5 and 6 are not implemented neither the AA_RESYNC primitives nor recognition of RS and RSAK PDUs is possible. NOTE 2 – If States 7, 8 and 9 are not implemented neither the AA_RECOVER primitives nor recognition of ES and ESAK PDUs is possible. NOTE 3 – Some of the connection control procedures make use of macros defined in Figure 22 (27 to 29 of 38).				

I.2.4.7.3 Assured data transfer procedure

Item number	Protocol Feature	Ref.	Status	Support
PAD1	Pre- and postprocessing procedures on receipt of POLL, STAT, and USTAT PDUs	Figure 22 (24 of 38)	M	
PAD2	Procedures after timer expiries	Figure 22 (25 of 38)	M	
PAD3	Procedures after "enabling conditions"	Figure 22 (25 of 38)	M	
PAD4	Procedures for sending an SD PDU	Figure 22 (30 of 38)	M	
PAD5	Procedures for processing a received SD PDU	Figure 22 (31 and 32 of 38)	M	
PAD6	Procedures for sending a POLL PDU	Figure 22 (33 of 38)	M	
PAD7	Procedures for processing a received POLL PDU	Figure 22 (33 of 38)	M	
PAD8	Procedures for sending a STAT PDU	Figure 22 (34 and 35 of 38)	M	
PAD9	Procedures for processing a received STAT PDU	Figure 22 (36 and 37 of 38)	M	
PAD10	Procedures for sending a USTAT PDU	Figure 22 (38 of 38)	M	
PAD11	Procedures for processing a received USTAT PDU	Figure 22 (38 of 38)	M	
NOTE – Some of the assured data transfer procedures make use of macros defined in Figure 22 (27 to 29 of 38).				

I.2.5 Supported values

I.2.5.1 Timers

This clause is applicable only if the major capability MC4 is implemented.

Item number	Item description	Ref.	Status	Support	Values	
					Allowed	Supported
T1	Timer_CC	8.6; Figure 22 (6, 10, 13 and 17 of 38)	M		(Note)	
T2	Timer_POLL	8.6; Figure 22 (25 of 38)	M		(Note)	
T3	Timer_KEEP-ALIVE	8.6; Figure 22 (25 of 38)	M		(Note)	
T4	Timer_NO-RESPONSE	8.6; Figure 22 (25 of 38)	M		(Note)	
T5	Timer_IDLE	8.6; Figure 22 (25 of 38)	M		(Note)	
T6	Timer_RESEQ	8.6; Figure 22 (25 of 38)	M		(Note)	
T7	Timer_GUARD	8.6; Figure 22 (2 of 38)	M		(Note)	
NOTE – This Recommendation does not specify any allowed values.						

I.2.5.2 Parameters for data transfer

Item number	Item description	Ref.	Status	Support	Values	
					Allowed	Supported
Assured data transfer						
P1	Maximum number of transmissions of a BGN, END, ER, or RS PDU ("MaxCC")	8.7; Figure 22 (6, 10, 13 and 17 of 38)	MC4 M else N/A		(Note 1)	
P2	Upper limit of transmitted SD PDUs before sending a POLL PDU ("MaxPD")	8.7; Figure 22 (30 of 38)	MC4 M else N/A		(Note 1)	
P3	Maximum number of list elements placed in a STAT PDU ("MaxSTAT")	8.7; Figure 22 (35 of 38)	MC4 M else N/A		(Note 1)	
P4	The maximum number of octets in the Information field of an SD PDU ("k")	8.2.4; 8.7	MC4 M else N/A		0 … 65'528	
P5	The maximum number of octets in the SSCOP-UU field of a BGN, BGAK, BGREJ, END, or RS PDU ("j")	8.2.4; 8.7	MC4 M else N/A		0 … 65'524	

Item number	Item description	Ref.	Status	Support	Values	
					Allowed	Supported
Unassured data transfer						
P6	The maximum number of octets in the Information field of an UD PDU ("k")	8.2.4; 8.7	MC5 M else N/A		0 … 65'528	
P7	The maximum number of octets in the Information field of an MD PDU ("k")	8.2.4; 8.7	MC6 M else N/A		0 … 65'528	
Assured and unassured data transfer						
P8	The maximum number of simultaneously supported links ("MaxLinks")	I.2.4; (Note 2)	MC4 or MC5 or MC6 M else N/A		(Note 1)	
NOTE 1 – This Recommendation does not specify either minimal required nor maximum allowed values. NOTE 2 – This Recommendation does not specify actions on attempted exceeding of this value.						

I.2.6 Support of Convergence Functions

I.2.6.1 Selection of Convergence Function Option

Item number	Item description	Ref.	Status	Support
CF1	Convergence function for SSCOPMCE above IP or UDP	Annex C	O.2	
CF2	Convergence function for SSCOPMCE above IP or UDP with Differentiated Services	Annex D	O.2	
CF3	Convergence function for SSCOPMCE above Ethernet	Annex E	O.2	
O.2	Optional, but, if chosen, support of only one of these items is required (Note)			
NOTE – If no option is chosen, SSCOPMCE is using AAL5 CP.				

I.2.6.2 Selection of underlying Service (IP or UDP)

This clause is applicable only if the convergence function option CF1 or CF2 is implemented.

Item number	Item description	Ref.	Status	Support
UL1	Does the Convergence Function rely on the services provided by IP	C.3.1 or D.3.1	O.3	
UL2	Does the Convergence Function rely on the services provided by UDP	C.3.2 or D.3.2	O.3	
O.3	Support of one and only one of these items is required			

I.2.6.3 Mapping between Convergence Function and IP

This clause is applicable only if the convergence function option CF1 and the underlying service option UL1 are implemented.

Item number	Item description	Ref.	Status	Support
MP1	Transmitter side setting of PRECEDENCE to binary "000" (Sub-field of Type of Service (TOS)-field, see C.3.1.1)	C.3.1.2; Table C.1; Figure C.2	M	
MP2	Transmitter side mapping of Cell Loss Priority (CPCS-LP) into DELAY (D)-bit of TOS-field. DELAY = 1 if CPCS-LP = 0, else DELAY = 0	C.3.1.2; Table C.1; Figure C.2	M	
MP3	Transmitter side setting of THROUGHPUT (T)-bit of TOS-field to binary "0"	C.3.1.2; Table C.1; Figure C.2	M	
MP4	Transmitter side setting of RELIABILITY (R)-bit of TOS-field to binary "0"	C.3.1.2; Table C.1; Figure C.2	M	
MP5	Transmitter side setting of MONETARY COST (M)-bit of TOS-field to binary "0"	C.3.1.2; Table C.1; Figure C.2	M	
MP6	Transmitter side setting of SPARE-bit of TOS-field (bit no. 8) to binary "0"	C.3.1.2; Table C.1; Figure C.2	M	
MP7	Transmitter side generation of IDENTIFICATION to be inserted into Identification-field (definition see C.3.1.1)	C.3.1.2; Table C.1; Figure C.2	M	
MP8	Transmitter side setting of RESERVED-bit of Flag-field (bit no. 1) to binary "0"	C.3.1.2; Table C.1; Figure C.2	M	
MP9	Transmitter side setting of DON'T FRAGMENT (DF)-bit of Flag-field (bit no. 2) to binary "0"	C.3.1.2; Table C.1; Figure C.2	M	
MP10	Transmitter side generation of TIME TO LIVE (TTL) to be inserted into Time to Live-field (definition see C.3.1.1)	C.3.1.2; Table C.1; Figure C.2	M	
MP11	Transmitter side setting of PROTOCOL (PROT) to decimal value "128" to be inserted into Protocol-field (definition see C.3.1.1)	C.3.1.2; Table C.1; Figure C.2	M	
MP12	Transmitter side setting of SOURCE ADDRESS to the IP address of the source node	C.3.1.2; Table C.1; Figure C.2	M	
MP13	Transmitter side setting of DESTINATION ADDRESS to the IP address of the destination node	C.3.1.2; Table C.1; Figure C.2	M	
MP14	Applicability of Option LOOSE SOURCE AND RECORD ROUTE (LSRR)	C.3.1.2; Table C.1; Figure C.2	O	

Item number	Item description	Ref.	Status	Support
MP15	Applicability of Option STRICT SOURCE AND RECORD ROUTE (SSRR)	C.3.1.2; Table C.1; Figure C.2	O	
MP16	Applicability of Option RECORD ROUTE (RR)	C.3.1.2; Table C.1; Figure C.2	O	
MP17	Applicability of Option TIMESTAMP	C.3.1.2; Table C.1; Figure C.2	O	
MP18	Passing DATA to IP up to the maximum size (65535 – IHL)	C.3.1.2; Table C.1; Figure C.2	M	
MP19	Receiver side mapping of DELAY (D)-bit of TOS-field into Cell Loss Priority (CPCS-LP). CPCS-LP = 0 if DELAY = 1, else CPCS-LP = 1	C.3.1.3; Figure C.3	M	
MP20	Receiver side ignores content of PRECEDENCE-, THROUGHPUT (T)-, RELIABILITY (R)-, MONETARY COST (M)-, SPARE (bit no. 8)-sub-fields/bits of TOS-field	C.3.1.3; Figure C.3	M	
MP21	Receiver side processing of SDU. Process SDU if PROT = 128 (decimal), else discard SDU	C.3.1.3; Figure C.3	M	
MP22	Accepting DATA from IP up to the maximum size (65535 – IHL)	C.3.1.3; Figure C.3	M	

I.2.6.4 Mapping between Convergence Function and UDP

This clause is applicable only if the convergence function option CF1 and the underlying service option UL2 are implemented.

Item number	Item description	Ref.	Status	Support
MP31	Transmitter side setting of PRECEDENCE to binary "000" (Sub-field of Type of Service (TOS)-field, see C.3.1.1)	C.3.2.2; Figure C.5	M	
MP32	Transmitter side mapping of Cell Loss Priority (CPCS-LP) into DELAY (D)-bit of TOS-field. DELAY = 1 if CPCS-LP = 0, else DELAY = 0	C.3.2.2; Figure C.5	M	
MP33	Transmitter side setting of THROUGHPUT (T)-bit of TOS-field to binary "0"	C.3.2.2; Figure C.5	M	
MP34	Transmitter side setting of RELIABILITY (R)-bit of TOS-field to binary "0"	C.3.2.2; Figure C.5	M	
MP35	Transmitter side setting of MONETARY COST (M)-bit of TOS-field to binary "0"	C.3.2.2; Figure C.5	M	
MP36	Transmitter side setting of SPARE bit of TOS-field (bit no. 8) to binary "0"	C.3.2.2; Figure C.5	M	
MP37	Transmitter side generation of IDENTIFICATION to be inserted into Identification-field (definition see C.3.1.1)	C.3.2.2; Figure C.5	M	

Item number	Item description	Ref.	Status	Support
MP38	Transmitter side setting of RESERVED-bit of Flag-field (bit no. 1) to binary "0"	C.3.2.2; Figure C.5	M	
MP39	Transmitter side setting of DON'T FRAGMENT (DF)-bit of Flag-field (bit no. 2) to binary "0"	C.3.2.2; Figure C.5	M	
MP40	Transmitter side generation of TIME TO LIVE (TTL) to be inserted into Time to Live-field (definition see C.3.1.1)	C.3.2.2; Figure C.5	M	
MP41	Applicability of Option LOOSE SOURCE AND RECORD ROUTE (LSRR)	C.3.2.2; Figure C.5	O	
MP42	Applicability of Option STRICT SOURCE AND RECORD ROUTE (SSRR)	C.3.2.2; Figure C.5	O	
MP43	Applicability of Option RECORD ROUTE (RR)	C.3.2.2; Figure C.5	O	
MP44	Applicability of Option TIMESTAMP	C.3.2.2; Figure C.5	O	
MP45	Passing DATA to IP up to the maximum size (65535 – IHL – UDP Header)	C.3.2.2; Figure C.5	M	
MP46	Receiver side mapping of DELAY (D)-bit of TOS-field into Cell Loss Priority (CPCS-LP). CPCS-LP = 0 if DELAY = 1, else CPCS-LP = 1	C.3.2.3; Figure C.6	M	
MP47	Receiver side ignores content of PRECEDENCE-, THROUGHPUT (T)-, RELIABILITY (R)-, MONETARY COST (M)-, SPARE (bit no. 8)-sub-fields/bits of TOS-field	C.3.2.3; Figure C.6	M	
MP48	Accepting DATA from IP up to the maximum size (65535 – IHL – UDP Header)	C.3.2.3; Figure C.6	M	

I.2.6.5 Mapping between Convergence Function and IP with Differentiated Services

This clause is applicable only if the convergence function option CF2 and the underlying service option UL1 are implemented.

Item number	Item description	Ref.	Status	Support
MP61	Transmitter side mapping of Cell Loss Priority (CPCS-LP) into DIFFERENTIATED SERVICES CODEPOINT (DSCP) of TOS-field. DSCP = "000000" if CPCS-LP = 1, else DSCP = "xxx000" with "xxx" greather than "000" (Type of Service (TOS)-field and Class Selector Codepoints, see D.3.1.1)	D.3.1.2; Table D.1; Figure D.2	M	
MP62	Transmitter side setting of CURRENTLY UNUSED-sub-field of TOS-field to binary "00"	D.3.1.2; Table D.1; Figure D.2	M	
MP63	Transmitter side generation of IDENTIFICATION to be inserted into Identification-field (definition see C.3.1.1)	D.3.1.2; Table D.1; Figure D.2	M	

Item number	Item description	Ref.	Status	Support
MP64	Transmitter side setting of RESERVED-bit of Flag-field (bit no. 1) to binary "0"	D.3.1.2; Table D.1; Figure D.2	M	
MP65	Transmitter side setting of DON'T FRAGMENT (DF)-bit of Flag-field (bit no. 2) to binary "0"	D.3.1.2; Table D.1; Figure D.2	M	
MP66	Transmitter side generation of TIME TO LIVE (TTL) to be inserted into Time to Live-field (definition see D.3.1.1)	D.3.1.2; Table D.1; Figure D.2	M	
MP67	Transmitter side setting of PROTOCOL (PROT) to decimal value "128" to be inserted into Protocol-field (definition see D.3.1.1)	D.3.1.2; Table D.1; Figure D.2	M	
MP68	Transmitter side setting of SOURCE ADDRESS to the IP address of the source node	D.3.1.2; Table D.1; Figure D.2	M	
MP69	Transmitter side setting of DESTINATION ADDRESS to the IP address of the destination node	D.3.1.2; Table D.1; Figure D.2	M	
MP70	Applicability of Option LOOSE SOURCE AND RECORD ROUTE (LSRR)	D.3.1.2; Table D.1; Figure D.2	O	
MP71	Applicability of Option STRICT SOURCE AND RECORD ROUTE (SSRR)	D.3.1.2; Table D.1; Figure D.2	O	
MP72	Applicability of Option RECORD ROUTE (RR)	D.3.1.2; Table D.1; Figure D.2	O	
MP73	Applicability of Option TIMESTAMP	D.3.1.2; Table D.1; Figure D.2	O	
MP74	Passing DATA to IP up to the maximum size (65535 – IHL)	D.3.1.2; Table D.1; Figure D.2	M	
MP75	Receiver side mapping of DIFFERENTIATED SERVICES CODEPOINT (DSCP) of TOS-field into Cell Loss Priority (CPCS-LP). CPCS-LP = 1 if DSCP = "000000", else CPCS-LP = 0	D.3.1.3; Figure D.3	M	
MP76	Receiver side ignores content of CURRENTLY UNUSED-sub-field of TOS-field	D.3.1.3; Figure D.3	M	
MP77	Receiver side processing of SDU. Process SDU if PROT = 128 (decimal), else discard SDU	D.3.1.3; Figure D.3	M	
MP78	Accepting DATA from IP up to the maximum size (65535 – IHL)	D.3.1.3; Figure D.3	M	

I.2.6.6 Mapping between Convergence Function and UDP with Differentiated Services

This clause is applicable only if the convergence function option CF2 and the underlying service option UL2 are implemented.

Item number	Item description	Ref.	Status	Support
MP91	Transmitter side mapping of Cell Loss Priority (CPCS-LP) into DIFFERENTIATED SERVICES CODEPOINT (DSCP) of TOS-field. DSCP = "000000" if CPCS-LP = 1, else DSCP = "xxx000" with "xxx" greather than "000" (Type of Service (TOS)-field and Class Selector Codepoints, see D.3.1.1)	D.3.2.2; Figure D.5	M	
MP92	Transmitter side setting of CURRENTLY UNUSED-sub-field of TOS-field to binary "00"	D.3.2.2; Figure D.5	M	
MP93	Transmitter side generation of IDENTIFICATION to be inserted into Identification-field (definition see D.3.1.1)	D.3.2.2; Figure D.5	M	
MP94	Transmitter side setting of RESERVED-bit of Flag-field (bit no. 1) to binary "0"	D.3.2.2; Figure D.5	M	
MP95	Transmitter side setting of DON'T FRAGMENT (DF)-bit of Flag-field (bit no. 2) to binary "0"	D.3.2.2; Figure D.5	M	
MP96	Transmitter side generation of TIME TO LIVE (TTL) to be inserted into Time to Live-field (definition see D.3.1.1)	D.3.2.2; Figure D.5	M	
MP97	Applicability of Option LOOSE SOURCE AND RECORD ROUTE (LSRR)	D.3.2.2; Figure D.5	O	
MP98	Applicability of Option STRICT SOURCE AND RECORD ROUTE (SSRR)	D.3.2.2; Figure D.5	O	
MP99	Applicability of Option RECORD ROUTE (RR)	D.3.2.2; Figure D.5	O	
MP100	Applicability of Option TIMESTAMP	D.3.2.2; Figure D.5	O	
MP101	Passing DATA to IP up to the maximum size (65535 – IHL – UDP Header)	D.3.2.2; Figure D.5	M	
MP102	Receiver side mapping of DIFFERENTIATED SERVICES CODEPOINT (DSCP) of TOS-field into Cell Loss Priority (CPCS-LP). CPCS-LP = 1 if DSCP = "000000", else CPCS-LP = 0	D.3.2.3; Figure D.6	M	
MP103	Receiver side ignores content of CURRENTLY UNUSED-sub-field of TOS-field	D.3.2.3; Figure D.6	M	
MP104	Accepting DATA from IP up to the maximum size (65535 – IHL – UDP Header)	D.3.2.3; Figure D.6	M	

I.2.6.7 Mapping between Convergence Function and Ethernet (this section applies if CF3 is supported)

This clause is applicable only if the convergence function option CF3 is implemented.

Item number	Item description	Ref.	Status	Support
MP111	Transmitter side PREAMBLE pattern	E.3.1; Figure E.2	M	
MP112	Transmitter side setting of START FRAME DELIMITER (SFD) to binary "10101011"	E.3.2; Figure E.2	M	
MP113	Transmitter side setting of DESTINATION ADDRESS to the Ethernet address of the destination node, or broadcast address, as appropriate	E.3.3; Figure E.2	M	
MP114	Transmitter side setting of SOURCE ADDRESS to the Ethernet address of the source node	E.3.3; Figure E.2	M	
MP115	Transmitter side setting of LENGTH/TYPE to the value 0x8100 (hexadecimal) indicating "802.1 Q Tag Type"	E.3.4; Figure E.1 Figure E.2	M	
MP116	Transmitter side setting of USER PRIORITY (3-bit sub-field within the Tag Control Information (TCI) field) according to the priority requested by the user expressed by PRECEDENCE/CLASS OF SERVICE	E.3.5; Figure E.2	M	
MP117	Transmitter side setting of CANONICAL FORMAT IDENTIFIER (CFI) to binary 0	E.3.5; Figure E.2	M	
MP118	Transmitter side setting of VIRTUAL LOCAL AREA NETWORK (VLAN) identifier (VID) as requested by the user	E.3.5; Figure E.2	M	
MP119	Transmitter side setting of LENGTH/MAC CLIENT TYPE to decimal 8900 (0x22C4) indicating client protocol SSCOPMCE	E.3.6; Figure E.2	M	
MP120	Transmitter side setting of SOURCE PORT according to the value requested by the user	E.5; Figure E.2	M	
MP121	Transmitter side setting of DESTINATION PORT according to the value requested by the user	E.5; Figure E.2	M	
MP122	Passing MAC CLIENT DATA to Ethernet Data Link from 42 up to 1500 octets (including source and destination port identifier, 2 octets each)	E.5; Figure E.2	M	
MP123	Receiver side PREAMBLE pattern	E.3.1; Figure E.3	M	
MP124	Receiver side detection of START FRAME DELIMITER (SFD) to binary "10101011"	E.3.2; Figure E.3	M	
MP125	Receiver side detection of DESTINATION ADDRESS if it matches the Ethernet address of the destination node, or broadcast address, as appropriate	E.3.3; Figure E.3	M	

Item number	Item description	Ref.	Status	Support
MP126	Receiver side detection of SOURCE ADDRESS	E.3.3; Figure E.3	M	
MP127	Receiver side detection of LENGTH/TYPE if it matches "802.1 Q Tag Type" (value 0x8100)	E.3.4; Figure E.1 Figure E.3	M	
MP128	Receiver side passing of contents of USER PRIORITY (3-bit sub-field within the Tag Control Information (TCI) field) as PRECEDENCE/CLASS OF SERVICE (3-bit user priority) to the user	E.3.5; Figure E.3	M	
MP129	Receiver side detection of CANONICAL FORMAT IDENTIFIER (CFI); has to be binary 0	E.3.5; Figure E.3	M	
MP130	Receiver side passing of VIRTUAL LOCAL AREA NETWORK (VLAN) identifier (VID) to the user	E.3.5; Figure E.3	M	
MP131	Receiver side detection of LENGTH/MAC CLIENT TYPE matching decimal 8900 (0x22C4) indicating client protocol SSCOPMCE	E.3.6; Figure E.3	M	
MP132	Receiver side passing of SOURCE PORT to the user	E.5; Figure E.3	M	
MP133	Receiver side passing of DESTINATION PORT to the user	E.5; Figure E.3	M	
MP134	Accepting MAC CLIENT DATA from Ethernet Data Link from 42 up to 1500 octets (including source and destination port identifier, 2 octets each)	E.5; Figure E.3	M	

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	**Switching and signalling**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	Global information infrastructure and Internet protocol aspects
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2002